

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-268550

(43)Date of publication of application : 20.09.2002

(51)Int.Cl. G09C 1/04
G09C 1/00
H04N 1/44

(21)Application number : 2001-067113 (71)Applicant : SEIKO INSTRUMENTS INC

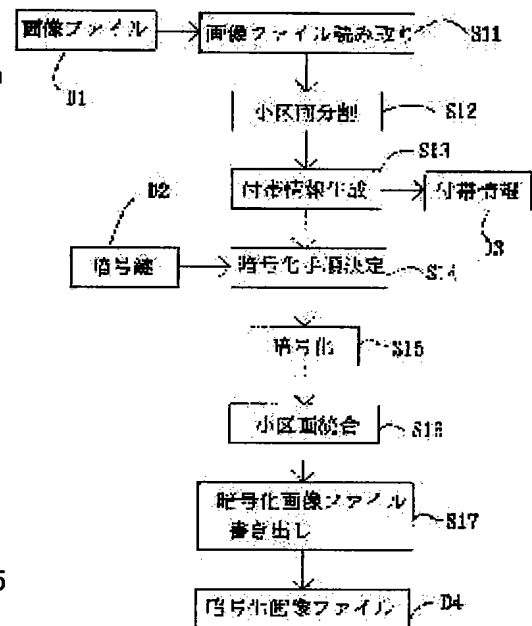
(22)Date of filing : 09.03.2001 (72)Inventor : ONO SHINSUKE

(54) IMAGE CIPHERING METHOD AND CIPHERING PROGRAM AND RECORDING MEDIUM STORING CIPHERED IMAGE FILE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an image ciphering method and ciphering program by which sketch information can be taken out from ciphered image information even without changing the existing method, device and procedure of image analysis, display, printing and sketch preparation at all.

SOLUTION: This method is provided with a first process S11 of inputting images by reading an image file indicating image information, a second process S12 of performing the optimum small section division of the images from the number of pixels of the image information and a specified parameter and generating accompanying information for the small section division, a third process S13 of replacing the pixels within the small section and performing ciphering for each small section by a prescribed ciphering procedure decided by a specified cipher key and fourth processes S14 and S15 of writing the ciphered image as a ciphered image file indicating the image information.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-268550
(P2002-268550A)

(43) 公開日 平成14年9月20日 (2002.9.20)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 9 C 1/04		G 0 9 C 1/04	5 C 0 7 5
	6 6 0	1/00	6 6 0 D 5 J 1 0 4
H 0 4 N 1/44		H 0 4 N 1/44	

審査請求 未請求 請求項の数16 O L (全 7 頁)

(21) 出願番号 特願2001-67113(P2001-67113)

(22) 出願日 平成13年3月9日 (2001.3.9)

(71) 出願人 000002325

セイコーインスツルメンツ株式会社
千葉県千葉市美浜区中瀬1丁目8番地

(72) 発明者 大野 伸介

東京都江東区亀戸6丁目31番1号 セイコー
アイテック株式会社内

(74) 代理人 100096378

弁理士 坂上 正明

Fターム(参考) 5C075 CD07 EE03 FF90

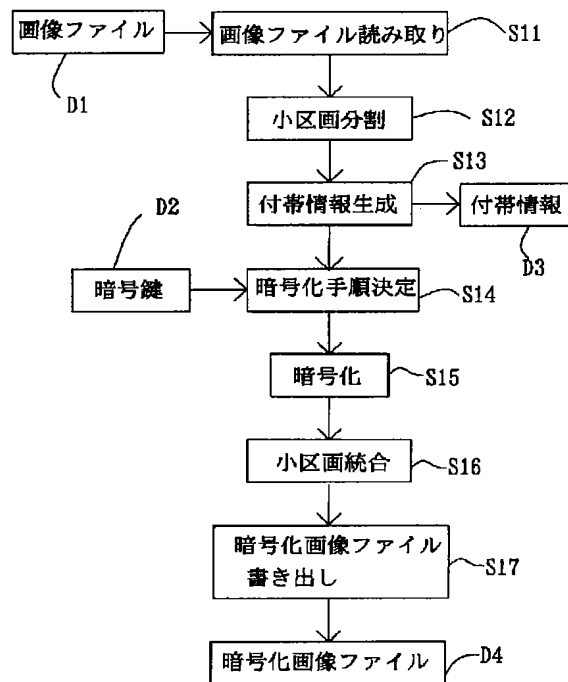
5J104 AA15 JA03 NA02 NA12

(54) 【発明の名称】 画像の暗号化方法及び暗号化プログラム並びに暗号化画像ファイルを格納した記録媒体

(57) 【要約】

【課題】 既存の画像の解析、表示、印刷、略図作成の方法・装置・手順に何ら変更を加えずとも、暗号化画像情報から略図情報を取り出すことを可能な画像の暗号化方法及び暗号化プログラムを提供する。

【解決手段】 画像情報を表す画像ファイルを読み取ることによって画像を入力する第1の工程S11と、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成する第2の工程S12と、指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行う第3の工程S13と、暗号化された画像を画像情報を表す暗号化画像ファイルとして書き出す第4の工程S14及びS15とを具備する。



【特許請求の範囲】

【請求項 1】 画像情報を表す画像ファイルを読み取ることで画像を入力する第 1 の工程と、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成する第 2 の工程と、指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行う第 3 の工程と、暗号化された画像を画像情報を表す暗号化画像ファイルとして書き出す第 4 の工程とを具備することを特徴とする画像の暗号化方法。

【請求項 2】 前記暗号鍵及び前記付帯情報に基づいて前記暗号化画像ファイルを復号化する第 5 の工程をさらに具備することを特徴とする請求項 1 に記載の画像の暗号化方法。

【請求項 3】 前記第 3 の工程での暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第 2 の付帯情報を生成することを特徴とする請求項 1 又は 2 に記載の画像の暗号化方法。

【請求項 4】 前記暗号化画像ファイルを復号化する際に前記第 2 の付帯情報を用いることを特徴とする請求項 3 に記載の画像の暗号化方法。

【請求項 5】 前記暗号化画像ファイルの形式が元の画像ファイルの形式と同一であることを特徴とする請求項 1 ～ 4 の何れかに記載の画像の暗号化方法。

【請求項 6】 コンピュータに、画像情報を表す画像ファイルを読み取ることで画像を入力する第 1 の手順と、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成する第 2 の手順と、指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行う第 3 の手順と、暗号化された画像を画像情報を表す暗号化画像ファイルとして書き出す第 4 の手順とを実行させることを特徴とする画像の暗号化プログラム。

【請求項 7】 前記第 3 の手順では暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第 2 の付帯情報を生成することを特徴とする請求項 6 に記載の画像の暗号化プログラム。

【請求項 8】 前記指定の暗号鍵を与えることにより、前記第 1 ～ 第 4 の手順を順次コンピュータに実行させることを特徴とする請求項 6 又は 7 に記載の画像の暗号化プログラム。

【請求項 9】 画像情報を表す画像ファイルと同一の構造を有し且つ当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成し且つ指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行うことにより生成される暗号化画像情報を表す暗号化画像ファイルを読

み取することで画像を入力する第 1 の手順と、前記付帯情報に基づいて当該画像の小区画分割を行うと共に前記指定の暗号鍵により決定される前記所定の暗号化手順により前記小区画毎に行う当該小区画内で画素を入れ替えを逆に行って復号化する第 2 の手順と、復号化された画像を画像情報を表す画像ファイルとして書き出す第 3 の手順とを、コンピュータに実行させることを特徴とする画像の復号化プログラム。

【請求項 10】 前記指定の暗号鍵及び前記付帯情報を与えることにより前記第 1 ～ 第 3 の手順を順次コンピュータに実行させることを特徴とする請求項 9 に記載の画像の復号化プログラム。

【請求項 11】 前記第 3 の手順は暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第 2 の付帯情報を生成するものであり、前記第 2 の手順では、前記第 2 の付帯情報を用いることを特徴とする請求項 9 又は 10 に記載の画像の復号化プログラム。

【請求項 12】 前記指定の暗号鍵、前記付帯情報及び前記第 2 の付帯情報を与えることにより前記第 1 ～ 第 3 の手順を順次コンピュータに実行させることを特徴とする請求項 11 に記載の画像の復号化プログラム。

【請求項 13】 請求項 6 ～ 12 の何れかのプログラムを記録したことを特徴とするコンピュータに読みとり可能な記録媒体。

【請求項 14】 画像情報を表す画像ファイルと同一の構造を有し、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成し且つ指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行うことにより生成される暗号化画像情報を表す構造を有する暗号化画像ファイルと、前記付帯情報を表す付帯情報データとを記録したことを特徴とするコンピュータに読みとり可能な記録媒体。

【請求項 15】 さらに、前記指定の暗号鍵を与えることにより当該暗号化画像ファイルを復号化する手順をコンピュータに実行させるプログラムを記録したことを特徴とする請求項 14 に記載のコンピュータに読みとり可能な記録媒体。

【請求項 16】 前記暗号化画像ファイルは、前記暗号化を所定の小区画についてのみ行われて生成されたものであり、当該所定の小区画についての第 2 の付帯情報を表すデータをさらに記録したことを特徴とする請求項 14 又は 15 に記載のコンピュータに読みとり可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、画像を暗号化し、また、暗号化された画像を復号化する画像暗号化方法、画像を暗号化し暗号化された画像を解読する装置、画像

を暗号化し暗号化された画像を解読する手順を記録した記録媒体に関する。

【0002】

【従来の技術】従来、画像の暗号化方法としては、特開平5-199424号公報及び特開平6-125553号公報に開示されているような方法が知られている。このような従来の暗号化方法により暗号化処理した後の暗号画像情報は、画像として表示することは一切できないため、どのような元画像であったかを推測することもできないという問題がある。また、特開2000-101853号に開示されているような方法では、略図を部分的に暗号化しないでおくことができるが、暗号化後の画像情報が一般的な画像形式でなくなるため、特別な方法・装置・手順でなければ暗号化画像から略図を取り出すことはできない。

【0003】

【発明が解決しようとする課題】上述したように、従来の暗号化処理方法では、暗号化処理した後の暗号画像情報は、一般の画像形式ではないので、復号化しなければ判読できない。従って、例えば、ウェブ上でコンテンツとして暗号化して画像を提供する場合には、サムネイルと呼ばれる縮小画像を添付する必要があるが、何れにしても、サムネイルとバラバラになってしまうと、復号化しない限り画像データの内容が判読できないという問題がある。

【0004】本発明は、このような事情に鑑み、既存の画像の解析、表示、印刷、略図作成の方法・装置・手順に何ら変更を加えずとも、暗号化画像情報から略図情報を取り出すことを可能な画像の暗号化方法及び暗号化プログラムを提供することを課題とする。

【0005】

【課題を解決するための手段】前記課題を解決する本発明の第1の態様は、画像情報を表す画像ファイルを読み取ることで画像を入力する第1の工程と、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成する第2の工程と、指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行う第3の工程と、暗号化された画像を画像情報を表す暗号化画像ファイルとして書き出す第4の工程とを具備することを特徴とする画像の暗号化方法にある。

【0006】本発明の第2の態様は、第1の態様において、前記暗号鍵及び前記付帯情報に基づいて前記暗号化画像ファイルを復号化する第5の工程をさらに具備することを特徴とする画像の暗号化方法にある。

【0007】本発明の第3の態様は、第1又は2の態様において、前記第3の工程での暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第2の付帯情報を生成することを特徴とする画像の暗号化方

法にある。

【0008】本発明の第4の態様は、第3の態様において、前記暗号化画像ファイルを復号化する際に前記第2の付帯情報を用いることを特徴とする画像の暗号化方法にある。

【0009】本発明の第5の態様は、第1～4の何れかの態様において、前記暗号化画像ファイルの形式が元の画像ファイルの形式と同一であることを特徴とする画像の暗号化方法にある。

10 【0010】本発明の第6の態様は、コンピュータに、画像情報を表す画像ファイルを読み取ることで画像を入力する第1の手順と、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成する第2の手順と、指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行う第3の手順と、暗号化された画像を画像情報を表す暗号化画像ファイルとして書き出す第4の手順とを実行させることを特徴とする画像の暗号化プログラムにある。

【0011】本発明の第7の態様は、第6の態様において、前記第3の手順では暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第2の付帯情報を生成することを特徴とする画像の暗号化プログラムにある。

【0012】本発明の第8の態様は、第6又は7の態様において、前記指定の暗号鍵を与えることにより、前記第1～第4の手順を順次コンピュータに実行させることを特徴とする画像の暗号化プログラムにある。

30 【0013】本発明の第9の態様は、画像情報を表す画像ファイルと同一の構造を有し且つ当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成し且つ指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行うことにより生成される暗号化画像情報を表す暗号化画像ファイルを読み取ることで画像を入力する第1の手順と、前記付帯情報に基づいて当該画像の小区画分割を行うと共に前記指定の暗号鍵により決定される前記所定の暗号化手順により前記小区画毎に行う当該小区画内で画素を入れ替えを逆行して復号化する第2の手順と、復号化された画像を画像情報を表す画像ファイルとして書き出す第3の手順とを、コンピュータに実行させることを特徴とする画像の復号化プログラムにある。

【0014】本発明の第10の態様は、第9の態様において、前記指定の暗号鍵及び前記付帯情報を与えることにより前記第1～第3の手順を順次コンピュータに実行させることを特徴とする画像の復号化プログラムにある。

50 【0015】本発明の第11の態様は、第9又は10の

態様において、前記第3の手順は暗号化を所定の小区画についてのみ行うと共に当該所定の小区画についての第2の付帯情報を生成するものであり、前記第2の手順では、前記第2の付帯情報を用いることを特徴とする画像の復号化プログラムにある。

【0016】本発明の第12の態様は、第11の態様において、前記指定の暗号鍵、前記付帯情報及び前記第2の付帯情報を与えることにより前記第1～第3の手順を順次コンピュータに実行させることを特徴とする画像の復号化プログラムにある。

【0017】本発明の第13の態様は、第6～12の何れかの態様のプログラムを記録したことを特徴とするコンピュータに読みとり可能な記録媒体にある。

【0018】本発明の第14の態様は、画像情報を表す画像ファイルと同一の構造を有し、当該画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行うと共に当該小区画分割についての付帯情報を生成し且つ指定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行うことにより生成される暗号化画像情報を表す構造を有する暗号化画像ファイルと、前記付帯情報を表す付帯情報データとを記録したことを特徴とするコンピュータに読みとり可能な記録媒体にある。

【0019】本発明の第15の態様は、第14の態様において、さらに、前記指定の暗号鍵を与えることにより当該暗号化画像ファイルを復号化する手順をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータに読みとり可能な記録媒体にある。

【0020】本発明の第16の態様は、第14又は15の態様において、前記暗号化画像ファイルは、前記暗号化を所定の小区画についてのみ行われて生成されたものであり、当該所定の小区画についての第2の付帯情報を表すデータをさらに記録したことを特徴とするコンピュータに読みとり可能な記録媒体にある。

【0021】かかる本発明によれば、暗号化した暗号化画像ファイルが、暗号鍵なしでも暗号化前の画像ファイルと同様に一般のアプリケーションで読み込むことができ、元の画像の概略を把握することができ。従って、暗号化した概略画像の著作権を解放することで、画像情報の著作権を持たない者が画像情報を複製保管配布しても、著作者の著作権の侵害に当該なくなり、画像検索システムを容易に構築できるなどの効果を奏する。

【0022】

【発明の実施の形態】以下、本発明を一実施形態に基づいて説明する。

【0023】図1には、一実施形態に係る暗号化方法の手順を示す。必要となるのは、暗号化プログラムと、JPEG、GIF、BMPなどの一般的な形式の画像ファイルD1及び暗号鍵D2であり、暗号化プログラムで画像ファイルD1を読み込み、暗号鍵D2を入力すること

により、所定の手順が実行されて暗号化画像ファイルD4が出力される。

【0024】まず、ステップS11で画像ファイルD1を読み込むと、画像情報の画素数と指定パラメーターから最適な画像の小区画分割を行う（ステップS12）。ここで、小区画分割はプログラムが自動的に判断するようにしてもよいし、設定できるようにしてもよく、画像の大きさによって、また、暗号化した後に概略がどの程度把握できるか（暗号化の強さ）によって決定すればよく、例えば、 8×8 、 16×16 、 8×16 、 64×64 等を挙げることができる。また、どのような小区分に分割したかについての付帯情報D3を生成する（ステップS13）。

【0025】次に、詳細は後述するが、所定の暗号鍵により決定される所定の暗号化手順により前記小区画毎に当該小区画内で画素を入れ替えて暗号化を行い（ステップS15）、小区画統合を行う（ステップS16）。暗号化された画像を画像情報を表す暗号化画像ファイルD4として書き出す（ステップS17）。ここで、暗号化手順の特長は、小区分内で画素を入れ替えることにより、暗号化を行うことであり、画像情報の形式に影響を与えず、また、暗号化後も画像の全体の雰囲気や色合いなどの概略が把握できるという利点がある。

【0026】本発明の暗号化プログラムは、図2に示すように、乱数発生アルゴリズム11及び暗号化手順アルゴリズム12を具備し、入力された暗号鍵D2を使用して乱数発生アルゴリズム11により乱数列13を得る。また、このようにして得られた乱数列13を用いて暗号化手順アルゴリズム12により、暗号化手順14を得る。

【0027】ここで、乱数発生アルゴリズム11は、一般的に知られている、DESなどの暗号アルゴリズムや、MD5、SHAなどの暗号学のハッシュであり、指定された暗号鍵D3より、図3に示すような所定の乱数列13を発生させる。この乱数列13は暗号鍵D3により一義的に決定されるが、逆に乱数列13から暗号鍵D3を予測することはできないとされている。

【0028】一方、暗号化手順アルゴリズム12は、乱数列13に基づいて所定の画素入れ替え手順を一義的に決定するものである。例えば、一区画区が 64×64 画素の場合の例であるが、乱数列13の最初から2桁ずつをとって64より大きいときは64を引いて64以内の数字を得、このように得た数字の上から2組ずつを画素入れ替え位置とし、このような画素入れ替えを所定の段数だけ、例えば、64段繰り返す、というものである。このようにして得られるのが、暗号化手順14である。

【0029】このようにして得られた暗号化画像ファイルD4は、画像ファイルD1と同一の画像形式であり、小区画毎に画素の入れ替えを行っただけなので、暗号鍵D2なしに、画像の概略を把握することができる。ま

た、暗号化プログラムに画像変換ソフトを組み込んで暗号化と同時に指定の画像形式に変換してもよいことは言うまでもない。

【0030】図4には、暗号化画像ファイルD4の復号化手順を示す。図4に示すように、まず、ステップS21で暗号化画像ファイルD4を読み込み、付帯情報D3に基づいて所定の小区画に分割する（ステップS22）。また、暗号化したときに使用した同一の暗号鍵D2を用いて復号化手順を決定する（ステップS23）。そして、復号化して（ステップS24）、小区画統合を行（ステップS25）、画像ファイルD5を出力する（ステップS26）。

【0031】ここで、復号化手順は、例えば、図2に示すような乱数発生アルゴリズム11及び暗号化手順アルゴリズム12が決定されていれば、暗号化手順の逆に画素の入れ替えを行う復号化手順を決定することができる。また、画像ファイルD5は、通常は暗号化される前の画像ファイルD1と同一形式であるが、暗号化の際に画像形式を変換していれば、変換された画像形式のファイルとなる。

【0032】以上説明した実施形態では、暗号化を分割された小区画の全体に対して小区画毎に行ったが、部分的な小区画のみに対して暗号化を行ってもよい。

【0033】この手順を図5に示す。この実施形態では、小区画分割を行った（ステップS12）の後、暗号化を行う小区画を決定し、第2の付帯情報D6を生成する（ステップS13A）。ここで、暗号化する小区画の決定は、プログラムが自動的に判断するようにしてもよいし、設定できるようにしてもよく、第2の付帯情報D6は、暗号化する小区画を特定できるものであれば、その形式は限定されない。なお、このような暗号化する小区画を決定する第2の付帯情報D6を生成する場合には、全体を暗号化する際には全体という情報を生成する必要がある。

【0034】また、このように暗号化された暗号化画像ファイルD4を復号化する手順を図6に示す。この場合、付帯情報D3に基づいて小区画に分割した後、第2の付帯情報D6により、復号化する小区画を特定し（ステップS22A）、その領域のみ復号化し（ステップS23）する。

【0035】このように画像の一部分のみを暗号化することにより、暗号化画像ファイルから、概略を把握し易いという効果を奏する。

【0036】以上説明した暗号化及び復号化の手順の全体を図7に示す。図1～図6と同一作用を示す部分には同一符号を付して説明は省略する。これによれば、画像ファイルD1の全体の概略が、暗号化された暗号化画像ファイルD4からも把握できることがイメージできる。また、画像ファイルD1がカラー画像であれば、小区画

毎の画素の入れ替えによる暗号化だから、全体の色合いのイメージも変化しないという利点もある。

【0037】このような暗号化方法は、既存の暗号アルゴリズムにより、暗号学的な強度が保証されるが、小区画毎に画素を入れ替えるだけであるという画像暗号化アルゴリズムにより、暗号化後も画像の概略を把握できるものである。

【0038】このような本発明の暗号化方法によれば、画像ファイルをCD-ROMなどのメディアを介して、又はウェブ上で閲覧、配布し、販売等する場合に、暗号化画像ファイルのみを閲覧させればよく、サムネイルファイルを付帯させる必要はない。また、暗号鍵がなくても暗号化画像ファイルのみから画像の概略が把握できるので、復号化しないと何の画像であるか不明である等の不都合がなくなる。

【0039】暗号化画像ファイルを閲覧、配布する際に、付帯情報（第2の付帯情報があればそれを含めて）を添付しておき、販売の際に暗号鍵を提示することにより、安全且つ容易に画像の閲覧、配布及び販売を行うことができる。また、この際、復号化するための暗号化プログラム又は復号化プログラムを同時に配布するようにすればよい。

【0040】

【発明の効果】以上説明したように、本発明によれば、既存の画像の解析、表示、印刷、略図作成の方法・装置・手順に何ら変更を加えずとも、暗号化画像情報から略図情報を取り出すことを可能な画像の暗号化方法及び暗号化プログラムを提供することができるという効果を奏する。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る暗号化の手順を示す図である。

【図2】本発明の一実施形態に係る暗号化の手順を説明する図である。

【図3】本発明の一実施形態に係る暗号化の手順を説明する図である。

【図4】本発明の一実施形態に係る復号化の手順を示す図である。

【図5】本発明の他の実施形態に係る暗号化の手順を示す図である。

【図6】本発明の他の実施形態に係る復号化の手順を示す図である。

【図7】本発明の暗号化及び復号化の手順を示す図である。

【符号の説明】

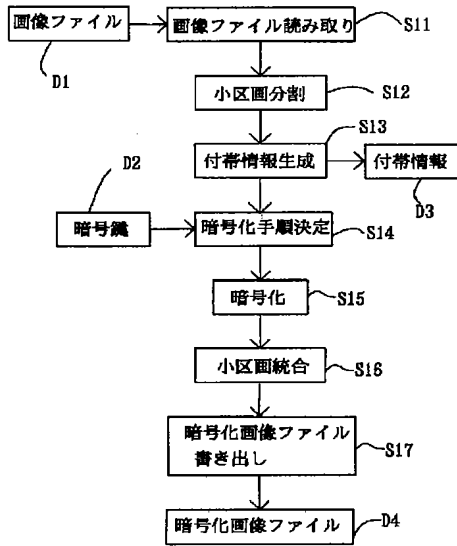
D1、D5 画像ファイル

D2 暗号鍵

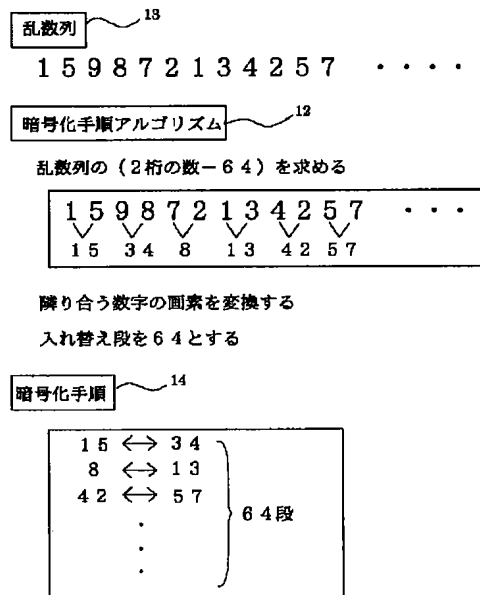
D3 付帯情報

D4 暗号化画像ファイル

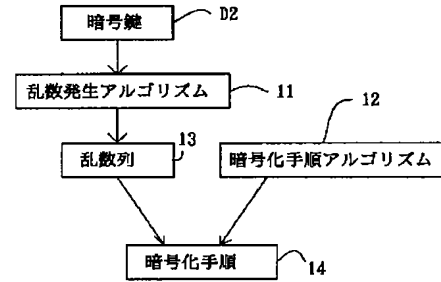
【図1】



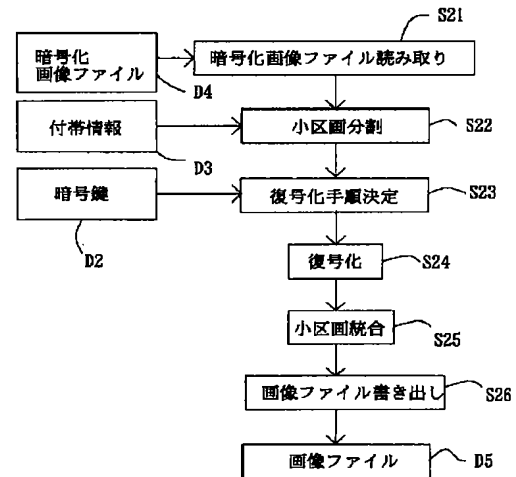
【図3】



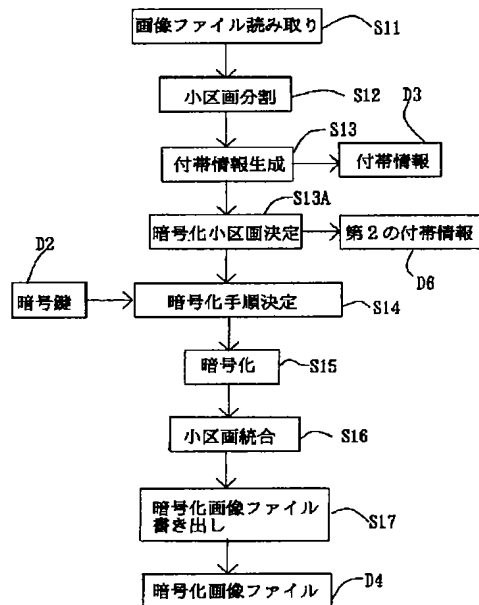
【図2】



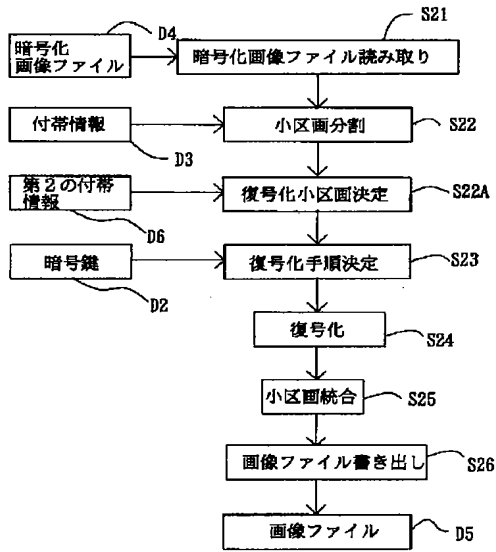
【図4】



【図5】



【図6】



【図7】

